LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoturvaohjeiden nykytilanne ja tulevaisuus

Leo Salonen

2018 Laurea

Laurea-ammattikorkeakoulu

Tietoturvaohjeiden nykytilanne ja tulevaisuus

Leo Salonen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Leo Salonen

Tietoturvaohjeiden nykytilanne ja tulevaisuus

Vuosi 2018 Sivumäärä 38

Valmet Automotive on autoteollisuuden johtava palveluntuottaja. Lähiaikana tapahtuneet isot rekrytoinnit ja yrityksen nopea kasvu asettavat haasteita turvallisuusjohtamiselle ja käyttäjien tietoturvallisuuden tietoisuuden ja koulutuksen kehittämiselle. Haasteita lisäävät myös teollisuuden kiristyvät vaatimukset sekä digitalisaatio.

Tämä opinnäytetyö on tapaustutkimus, jonka tutkimusaineisto on kerätty dokumenttianalyysi -menetelmällä. Työn tavoitteena on tutkia tietoturvallisuuteen liittyvien ohjeiden nykytilannetta ja verrata nykyisiä ohjeita yritykseen asetettuja vaatimuksia vasten. Vaatimukset koostuvat lainsäädännöstä ja yleisesti toimialalla käytettävistä standardeista. Tämän lisäksi tietoperustassa käsitellään turvallisuusjohtamiseen liittyvää kirjallisuutta. Turvallisuuskulttuuri on osa turvallisuusjohtamista, joka ohjaa turvallisuustyön toteuttamista. Lukijan on keskeistä ymmärtää, että voimassa olevat vaatimukset ovat jatkuvasti kiristyviä ja ne vaativat jatkuvaa prosessien parantamista.

Nykytilanne yrityksen ohjeistuksessa on hyvä, mutta ohjeiden jalkauttamisessa osaksi toimintaa sekä ohjeiden saatavuudessa käyttäjälle on haasteita. Ohjeiden on oltava käyttäjien saatavilla, jotta käyttäjät pystyvät tarkastamaan heitä kohtaan asetetut vaatimukset ja vastuut. Tämän lisäksi kehitettävinä kohteina on mobiililaitteiden ja etätyöohjeiden päivittäminen sekä niihin liittyvien prosessien kehittäminen.

Opinnäytetyön perusteella yrityksessä on käynnistetty korjaavat toimenpiteet, joiden tavoitteena on työn kehitysehdotuksissa esiin nousseiden kohteiden parantaminen. Työn eri vaiheissa esiin nousi myös muitakin kehittämiskohteita, mutta nämä on jätetty tämän opinnäytetyön ulkopuolelle.

Asiasanat: Käyttäjä, Tietoturvallisuusohjeet, Tietoturvallisuusvaatimukset

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor´s Degree

Leo Salonen

The current situation and the future of information security guidelines

Year 2018 Pages 38

Valmet Automotive is the leading service provider in the automotive industry. The recent recruitment and rapid growth in the company pose challenges for security management and the development of awareness and training on users' information security skills. Challenges are also heightened by intensified industry demands and digitalisation.

This thesis is a case study and the research materials were collected using the documental analysis method. The objective of the thesis is to study the current state of the information security guidelines and to compare existing guidelines against the requirements of the company. The requirements consist of legislation and general industry standards. In addition, literature on safety management is discussed in the theoretical framework. Security culture is a part of security leadership that guides the implementation of security work. It is essential for the reader to understand that the requirements in force are constantly tightening and require a continuous improvement of processes.

The current situation of the company's guidelines is solid, but introducing the instructions for action as well as accessing the instructions by the user is a challenge. The guidelines must be accessible to users so that they can check their requirements and responsibilities. In addition to this, other matters to be developed are the updating of mobile devices and telecommunications manuals and the development of related processes.

Based on the thesis, remedial measures have been initiated in the company with the aim of improving the targets highlighted in the development proposals. At other stages of the work, other areas of development also emerged, but these have been excluded from this thesis.

Keywords: Information Security Guidelines, Information security Requirements, User

Sisällys

1 Johdanto

Toiminnan kehittäminen kuuluu osaksi jokaisen työntekijän tehtäviä. Yrityksen toiminnoissa kehittämistyön merkitys on nopeasti kasvanut, koska maailma muuttuu nopeammin ja yrityksen tulee pysyä kehityksen mukana. Jatkuva kehittäminen on tekijä, joka erottaa menestyneen yrityksen muuttuvassa ja digitalisoituvassa toimintaympäristössä. (Ojasalo, Moilanen, Ritalahti 2014, 11–13.) Käyttäjän tietoturvallisuustietoisuus on puolestaan tekijä, joka tukee tietoturvallisuuden kehittämistä. Tietävä käyttäjä pystyy raportoimaan poikkeamista, joita tietämätön käyttäjä havainnoi.

Teollisuudessa on jatkuvasti kiristyvät tietoturvallisuusvaatimukset, jotka vaativat käyttäjien jatkuvaa tietoturvallisuustietoisuuden kehittämistä. Tieto- ja kyberturvallisuus muuttuu jatkuvasti muun maailman mukana. Yrityksen on suojattava omia tietojaan, ja lisäksi yrityksellä on velvollisuus suojata sen asiakkaiden tietoja ja työntekijöiden henkilötietoja.

Tämän opinnäytetyön tutkimusstrategiana on tapaustutkimus, koska tarkoituksena on tutkia syvällisesti muutamaa ilmiökokonaisuutta (Jyväskylän Yliopisto, 2015). Tavoitteena on selvittää Valmet Automotiven tietoturvaohjeiden nykytilanne sekä verrata nykytilannetta voimassaoleviin asiakasvaatimuksiin, standardeihin sekä asetuksiin. Työn tuloksena on kuvaus nykytilanteesta ja kehitysehdotukset.

Opinnäytetyölle asetetut tutkimuskysymykset ovat:

1. Mikä on tietoturvallisuusohjeiden nykytilanne?

2. Mitä tietoturvaohjeita käyttäjät tarvitsevat ja miksi?

Työ on tehty Laurea-Ammattikorkeakoulun (2017) opinnäytetyön ohjeen mukaisesti. Opinnäytetyössä esitellään aluksi Valmet Automotiven organisaatio, jotta lukija saa peruskäsitteet ja -käsityksen yrityksen toimintatavasta. Tämän jälkeen kuvataan opinnäytetyön tietoperusta käyttäjien tarvitsemille ohjeille. Osio sisältää keskeiset käsitteet ja toimintaa ohjaavat vaatimukset. Tietoperustan pohjalta suoritetaan nykytila-analyysi, jonka perusteella määritellään kehitysehdotukset.

2 Opinnäytetyön toimeksiantaja

Valmet Automotive on opinnäytetyön toimeksiantaja, ja työ toteutetaan yhteistyössä informaatiotekniikkaosaston ja turvallisuusosaston kanssa. Tässä osiossa käsitellään Valmet Automotiven historiaa ja toimintaa sekä opinnäytetyön kannalta tärkeiden osastojen esittelyä. Osion tavoitteena on, että lukija ymmärtää organisaation rakenteen ja toimintaympäristön, jotta hän pystyy analysoimaan opinnäytetyön tuloksia.

2.1 Valmet Automotive

Valmet Automotive on johtava autoteollisuuden palveluntuottaja. Yritys tarjoaa valmistus- ja suunnittelupalveluja, liiketoimintapalveluja sekä avoautojen kattojärjestelmiä. Yrityksen palveluksessa on yli 5000 osaajaa Suomessa, Saksassa, Puolassa ja Espanjassa. Nykyiset valmistettavat automallit Uudenkaupungin autotehtaalla ovat Mercedes Benzin A-sarja ja GLC katumaasturi. Yritys on valmistanut yli 1,2 miljoonaa autoa ja on näin yksi maailman suurimpia autoteollisuuden sopimusvalmistajia. Yrityksellä on kolme liiketoimintalinjaa: valmistusliiketoiminta, suunnittelutoiminta ja kattojärjestelmät. (Valmet Automotive 2017 a.)

Valmet Automotiven autotehdas on perustettu vuonna 1968 Saab-Valmet nimisenä yrityksenä yhteistyössä Valmetin ja ruotsalaisen Saab-Scanian välillä, ja yhtiön tavoitteena tuolloin oli autoteollisuuteen liittyvän osaamisen tuominen Suomeen sekä työn tarjoaminen työntekijöille. Ensisijainen tarkoitus oli valmistaa ajoneuvoja kotimaiselle markkinalle, mutta toiminnan laatu ja joustavuus avasivat ovet myös vientimarkkinoille. (Valmet Automotive 2017 b.)

Vuosi 2017 oli yritykselle merkittävän kasvun vuosi. Yritys vahvisti suunnitteluosaamistaan merkittävällä yritysostolla Saksasta. Yritysosto nosti suunnittelupalveluiden henkilöstömäärän yli 1 000 henkilöön. Kasvusta kertoo paljon myös se, että tammikuussa 2017 Uudenkaupungin autotehtaalla työskenteli 1900 työntekijää, kun tätä opinnäytetyötä tehtäessä työtekijöitä on jo noin 3500. Lisäksi tehdas on siirtynyt ensimmäistä kertaa historiassa kolmeen vuoroon kuutena päivänä viikossa. (Valmet Automotive 2017 c.) Suuresta henkilömäärästä johtuen koulutustaso on vaihtelevaa, ja lisäksi useat eri kansallisuudet tuovat omat haasteensa tietoturvallisuuden kouluttamiseen.

Yrityksen tulevaisuus näyttää positiiviselta. Helmikuussa 2017 julkaistiin, että Valmet Automotive alkaa valmistaa seuraavan sukupolven kompaktiautomallia vakiinnuttaen näin autotehtaan tuotannon useiksi vuosiksi eteenpäin (Valmet Automotive, 2017 d).

2.2 Turvallisuusosasto

Turvallisuusosasto vastaa yrityksen ympäristö-, työ ja kokonaisturvallisuudesta. Myöhemmin käytetään lyhennettä HSE-osasto, joka tulee englannin kielisistä sanoista Health, Safety and Environment. Osaston tärkein tehtävä on ohjata ja tukea liiketoimintalinjojen toimintaa omalla vastuualueellaan. Osasto on poikkiorganisatorinen, joten osasto toimii näköalapaikka-

na yrityksen eri toimintoihin. HSE-osasto raportoi tukiosaston johtajalle, joka puolestaan raportoi valmistusliiketoiminnan johtajalle. Yrityksellä on OHSAS 18001 työterveys- ja työturvallisuuden johtamisjärjestelmäsertifikaatti ja ISO 14001 Ympäristösertifikaatti.

HSE-osasto koostuu turvallisuusjohtajasta, työturvallisuusinsinööristä, ympäristöinsinööristä, kahdesta turvallisuusasiantuntijasta ja tietoturvapäälliköstä. Yksikön tehtävänä on suojata yritykselle tärkeitä arvoja, kuten henkilöitä, omaisuutta, ympäristöä ja mainetta sekä edistää yrityksen kilpailukykyä ja parantaa tuottavuutta. Tavoitteena osastolla on tukea yrityksen strategian toteutumista ja mahdollistaa yrityksen toiminta kaikissa tilanteissa.

Tietoturvallisuuden osalta yrityksessä on tehty vastuujako, jossa HSE-osasto vastaa turvallisuusjohtamisesta ja fyysisestä tietoturvallisuudesta, ja Informaatiotekniikkaosasto teknisestä tietoturvallisuudesta. Turvallisuusjohtamisen tavoitteena on riittävä valmius ja kyvykkyys yrityksen turvalliseen toimintaan normaalioloissa ja poikkeustapauksissa. Fyysisen tietoturvallisuuden tavoitteena on varmistaa salassa pidettävien tietojen eheys, luottamuksellisuus ja saatavuus. Turvallisuuden toteuttaminen on yhteistyötä eri osastojen välillä. Tekninen tietoturvallisuus on informaatiotekniikkaosaston vastuulla, mutta toimintaa hoidetaan yhdessä, jolloin toimintaa tarkastellaan eri osastojen toimesta.

2.3 Informaatiotekniikkaosasto

Informaatiotekniikkaosasto (myöhemmin käytetään lyhennettä IT-osasto) on talousjohtajan hallinnassa oleva yksikkö. Osaston tehtävänä on vastata IT-järjestelmien toiminnasta, ylläpidosta ja kehittämisestä sekä järjestelmien toiminnasta kaikissa tilanteissa. IT-osastoa johtaa tietohallintojohtaja, ja osastoon kuuluu 20 henkilöä eri liiketoimintalinjoista. Osasto on poikkiorganisatorinen, ja se raportoi kokonaisuudesta talousjohtajalle ja liiketoimintalinjojen toiminnasta liiketoimintalinjojen johtajille. Tietoturvallisuuden osalta IT-osasto vastaa teknisen tietoturvallisuuden toteuttamisesta, valvonnasta ja vaatimustenmukaisuudesta. IT-osaston organisaatio rakennetta ei kuvata opinnäytetyössä tarkemmin.

2.4 Laatuosasto

Laatuosasto on osa valmistusliiketoiminnan tukiosastoa. Laatuosasto raportoi toiminnastaan tukiosaston johtajalle. Osaston tehtäviin kuuluvat tuotelaatu, johtamisjärjestelmä ja auditoinnit sekä laadun kehitys. Osastolle kuuluu 10 työtekijää, ja sen tehtävänä on tarkastella laatua isossa kuvassa valmistusliiketoiminnassa. Tämän lisäksi laadun valvontaa ja kehittämistä tekee kokoonpanon organisaatiossa oleva laatuyksikkö. Yrityksellä on ISO 9001 laadunhallintajärjestelmän sertifikaatti.

Opinnäytetyön kannalta laatuosaston käsittely on relevanttia, koska laatuosaton vastuulla on johtamisjärjestelmät ja sisäisten sekä ulkoisten auditointien kehittäminen ja valvonta. Tur-

vallisuustoiminnalla ja laadunvarmistuksella on sama tavoite: häiriötön toiminta, jonka lopputuotteena on korkea asiakastyytyväisyys (Leppänen 2006, 26).

3 Opinnäytetyön tietoperusta

Opinnäytetyön tietoperusta eli käsitejärjestelmä ja toimintaa ohjaavat vaatimukset luovat lukijalle tietoisuuden yrityksen toimintaa ohjaavista vaatimuksista. Keskeiset käsitteet avaavat myös opinnäytetyön terminologiaa. Viitekehyksen ymmärtäminen mahdollistaa lukijalle työhön valittujen menetelmien ja valintojen sekä kehitysehdotusten arvioimisen. Käsitteistö on keskeinen yhteentoimivuuden osatekijä. (Avoin tiede ja tutkimus 2017.)

Tietoperusta käsittelee keskeiset käsitteet, tietoturvallisuuden hallinnan, turvallisuusjohtamisen, asiakasvaatimukset sekä toimintaa ohjaavan lainsäädännön. Tietoperusta on muodostettu tutkimalla voimassa olevia asiakassopimuksia, lainsäädäntöä ja valtionhallinnan tieto- ja kyberturvallisuuden johtoryhmän ohjeita sekä Juha Leppäsen kirjaa ”Yritysturvallisuus käytännössä”. Kirjassa avataan käytännönläheisesti turvallisuuden eri osa-alueet ja niiden kehittäminen. Keskeisenä vaatimuksena on standardi ISO 27001 (2017), joka määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset. Asiakasvaatimukset perustuvat standardiin ISO 27001.

3.1 Keskeiset käsitteet

Keskeiset käsitteet on kuvattu opinnäytetyön tietoperustasta valitsemalla käsitteet, jotka lukijan on hyvä ymmärtää. Käsitteiden ymmärtäminen antaa lukijalle myös mahdollisuuden tarkastella työn tuloksia, johtopäätöksiä ja kehitysehdotuksia.

Tiedolla tarkoitetaan liiketoiminnalle tärkeää suojattavaa kohdetta ja siksi sitä on suojattava asianmukaisesti. Tietoa voi olla monenlaisissa muodoissa paperilla, tietojärjestelmissä ja työntekijöillä aineettomana tietona. Täten tietoa voidaan myös siirtää eri muodoissa, joten jokaiseen muotoon tarvitaan omanlainen suojaus, jotta voidaan varmistaa tiedon suojauksen asianmukaisuus. (ISO 27000 2017.) Tieto, jota ei ole pyritty pitämään salassa ja johon ei ole kohdistettu tosiallista salassapitotoimenpiteitä, ei nauti yrityssalaisuuden suojaa yritysvakoilun tai yrityssalaisuuden rikkomisen, paljastamisen ja väärinkäytöksen varalta. (Leppänen 2006, 273).

Tietoturvallisuus on keskeinen osa organisaation turvallisuutta. Tietoturvallisuus tarkoittaa tietojen luottamuksellisuuden, käytettävyyden ja eheyden takaamista, mutta teknologian kehitys edellyttää menetelmien jatkuvaa seuraamista ja toimenpiteiden kehittämistä. Tietoturvallisuudessa tulee panostaa toiminnan jatkuvuuden varmistamiseen, koska täydellistä turvallisuutta on mahdotonta saavuttaa. (Elinkeinoelämän keskusliitto 2016.)

Tietoturvallisuuden tavoitteena on tunnistaa yrityksen toiminnan kannalta merkittävät tiedot ja määritellä niille suojausprosessit, jotka kattavat koko tiedon elinkaaren ajan. Salassa pidettävä tieto muodostuu kolmesta osa-alueesta: 1. Salassapitotahto (Pyrkimys pitää tieto suojattuna), 2. Salassapitointressi (Tiedon ilmitulon vahingoittava vaikutus toiminnalle) 3. Tosiasiallinen salassapito (toimenpiteet, joilla tieto on pyritty salaamaan). (Leppänen 2006, 237, 287.)

Riskienhallinta tarkoittaa koordinoitua toimintaa, jolla yritystä johdetaan sekä ohjataan riskien osalta. Riskienhallintaprosessi tulee olla määritelty, jotta prosessille asetetut tavoitteet voidaan saavuttaa. Prosessi koostuu riskien tunnistamisesta, riskianalyysistä ja riskien merkityksen arvioinnista. (ISO 27000 2017.)

3.2 Tietoturvallisuuden hallinta

Tietoturvallisuuden hallinnalla tarkoitetaan organisaation rakenteiden toimintaa, jolla yrityksen tietoturvatoimenpiteitä ohjataan sekä toimintaa valvotaan ja jatkuvasti parannetaan. Hallinnan tulee perustua ylimmän johdon asettamiin tavoitteisiin ja kontrolleihin, jotka varmistavat tavoitteisiin pääsemisen. Riskienhallinta on tietoturvallisuuden hallinnan perusta, jotta turvallisuustoimenpiteet kohdistetaan toiminnan kannalta tarpeellisiin toimintoihin. Riskienhallinnassa tulee käyttää tietoturvallisuuden asiantuntijoita. Hallintarakenteet ovat yrityskohtaisia, mikä tarkoittaa, että toisen yrityksen hallintamallia ei voida suoraan siirtää toisen yrityksen käyttöön. Hallinta kattaa toiminnot, joilla varmistetaan tavat tai käytännöt, joilla resursseja ohjataan, käsitellään, valvotaan ja johdetaan. (ISO 27001 2017.)

Valtionvarainministeriön ohjeessa määritellään, että tietojärjestelyjen tarkoituksena on varmistaa tietoaineiston, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon. Käytännössä tämä merkitsee mm. sitä, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen saatavilla. Sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään. Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muiden vahinkojen, tapahtumien tai häiriötilanteiden vuoksi. Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin, kun niitä tarvitaan. Etenkin sähköisissä asiointipalveluissa tarve käyttää palveluita ympärivuorokautisesti ja paikasta riippumatta on lisääntynyt, kun käyttötavat ovat muuttuneet. Palveluiden täytyy kyetä tunnistamaan käyttäjät luotettavasti sekä tuottamaan tarvittavaa lokia, josta tapahtumat voidaan tarvittaessa jälkikäteen selvittää. (Vahti 2013.)

Hallintajärjestelmä tukee yrityksen tavoitteiden saavuttamista käytössä olevien organisaatiorakenteiden puitteissa. Hallintajärjestelmä antaa yritykselle valmiudet vastata asiakkaiden ja muiden sidosryhmien tietoturvavaatimuksiin, parantaa suunnitelmia ja toimintoja, toteuttaa yrityksen tietoturvatavoitteet, toimia asiakasvaatimusten ja lainsäädännön mukaisesti sekä hallita tieto-omaisuutta organisoidulla tavalla ja näin edistää jatkuvaa parantamista. Hallintajärjestelmän tulee olla linjassa yrityksen tavoitteiden kanssa, jotta järjestelmää on mahdollista toteuttaa ja jotta se tukee tavoitteiden saavuttamista. Tietoturvallisuuteen vaikuttavat tekijät ovat jatkuvassa muutoksessa. Järjestelmän tulee olla osa johtamis- ja hallintarakenteita sekä prosesseja, jotta toiminta on jatkuvaa ja ulottuu jokaisen toiminnan osaksi. Organisaation tulee ymmärtää oma sisäinen ja ulkoinen toimintaympäristö sekä sidosryhmien tarpeet ja odotukset, jotta tietoturvallisuuden hallintajärjestelmä on osa kokonaisuutta. (ISO 27001 2017.)

Hallintajärjestelmä rakentuu eri osakokonaisuuksista (ISO 27001 2017), joita ovat seuraavat: tietoturvapolitiikka, tietoturvallisuuden organisointi, henkilöstöturvallisuus, suojattavan omaisuuden hallinta, pääsynhallinta, salaus, turva-alueet, käyttöturvallisuus, viestintäturvallisuus, järjestelmän hankinta, kehittäminen ja ylläpito, suhteet toimittajiin, tietoturvahäiriöiden hallinta ja liiketoiminnan jatkuvuuden hallintaan liittyvät tietoturvanäkökohdat ja vaatimuksenmukaisuus. Työssä käsitellään käyttäjän ohjeiden näkökulmasta tarpeelliset kohdat.

Tietoturvallisuuden hallinnassa voidaan käyttää ISO-standardien mukaisen kehittämisen prosessia, joka sisältää suunnitteluvaiheen, toteutusvaiheen, tarkistusvaiheen ja kehitysvaiheen. Prosessin toiminta vaatii aktiivista toteutusta, jotta yritys saavuttaa toiminnan jatkuvan parantamisen. (VAHTI 2007, 38–39.) Kehittämisen prosessi käsitellään tarkemmin osana laadunhallintajärjestelmäosioita sekä kuviossa kolme.

Tietoturvallisuusohjeet ovat yksi tietoturvallisuuden hallinnan ilmentymistä. Voimassa olevat ja ajantasaiset sekä saatavilla olevat ohjeet kehittävät henkilöstön tietoisuutta ja osoittavat yrityksen sitoutumista tietoturvallisuuden toteuttamiseen. Mikäli yrityksessä ei ole ohjeita käyttäjille, käyttäjät eivät tiedä miten tulee toimia. Hallintamallin toimimattomuus taas tarkoittaa, että politiikassa asetettuja tavoitteita ei voida saavuttaa. Ohjeet kuvaavat myös tietoturvallisuuskulttuurin tasoa.

Järvinen & Rousku (40, 2017) toteavat että sataprosenttisen turvallista ratkaisua ei voida käytännössä koskaan rakentaa. Vaakakupissa ovat käytettävyys ja turvallisuus. Käytettävyyden ja turvallisuuden välillä joudutaan tekemään kompromisseja, joiden tulee olla linjassa yrityksen tavoitteiden ja mittareiden kanssa

3.3 Riskienhallinta ja turvallisuusjohtaminen

Riskienhallinta ja turvallisuusjohtaminen ovat osa johtamistapaa, joka tulee huomioida päätöksenteossa. Yrityksen strategia on turvallisuusjohtamisen perusta. Turvallisuus on yksilön kokemus tunteena, toisaalta toiminta, joka mahdollistaa turvallisuuden tunteen. Tunteeseen vaikuttaa tietämys riskeistä ja niihin liittyvistä todennäköisyyksistä. Turvallisuusjohtamisen kokonaisuuden muodostavat turvallisuuden eri osa-alueet, joista yhtenä osa-alueena on tietoturvallisuus. (Leppänen 2006, 52, 54 & 57.) Turvallisuutta ja riskienhallintaa pitää käsitellä mahdollistajana, joka mahdollistaa toiminnan kaikissa tilanteissa ja poikkeustilanteista mahdollisimman nopean toipumisen. On hyvä kuitenkin huomioida, että yritystoiminnan tavoitteet eivät ole kaikki kaikessa, vaan myös universaaleja arvoja, kuten ihmiset, elinympäristö ja kestävä kehitys on huomioitava yrityksen toiminnassa (Leppänen 2006, 175).

Riskienhallinnan tavoitteena on ensisijaisesti mahdollistaa perusliiketoimintakonseptin onnistuminen ja toiseksi varmistaa, että toteuttamiseen ja ylläpitämiseen liittyvät riskit pysyvät hallinnassa. Riskin ottaminen on osa liiketoiminnan perusluonnetta. (Leppänen 2006, 23.) Riskejä käsitellessä on ymmärrettävä, mitä riskillä tarkoitetaan. Leppänen (2006, 30) määrittelee riskin tarkoittavan vaaraa tai yllättävää tapahtumaa, joka kielteisellä tavalla estää realisoituessaan kokonaan tai väliaikaisesti jonkin tavoitteen toteutumisen. On hyvä huomioida, että riski voi olla myös positiivinen. Riskin negatiiviset vaikutukset voidaan joissain tapauksissa ainakin osittain siirtää vakuutusyhtiölle, jolloin riskin realisoituminen ei ole yritykselle enää niin negatiivinen tapahtuma kuin aiemmin. Vakuutusyhtiölle vakuutetun riskin toteutuminen on negatiivinen, koska yhtiö joutuu korvaamaan vahingosta aiheutuneita kuluja sopimuksen mukaan. (Leppänen 2006, 41.) Riskejä käsiteltäessä riskin realisoitumisen vakuuttaminen pitää suhteuttaa yrityksen toimintaan, ja vakuutusten tulee perustua olemassa oleviin riskeihin. Vaikka riskinottaminen on osa liiketoimintaa, on yrityksen tunnistettava ne riskit, joita halutaan ottaa. Samalla on luonnollisesti varauduttava myös riskeihin, joita ei tiedetä.

Turvallisuusjohtamisen tavoitteena on, että sisäiset tai ulkoiset riskit eivät vaaranna yrityksen strategian toteuttamista. Voidaan sanoa, että turvallisuustoiminnan tehtävänä on varmistaa ja mahdollistaa ydinprosessin toteutuminen kaikissa tilanteissa. Vain tavoitteiden saavuttamiseen sekä varmistamiseen tähtäävä toiminta on tärkeää turvallisuusjohtamisessa. Kaikki sellainen toiminta, mikä ei johda tavoitteiden saavuttamiseen tai niiden varmistamiseen, on turhaa. Suojattavien kohteiden ja prosessien huolellinen määrittely varmistaa turvallisuuden ja riskienhallinnan kohdistamisen oikeisiin prosesseihin. Turvallisuusjohtaminen epäonnistuu, mikäli toiminta ei tue ydinprosessien toimintaa. Liiketoiminnan on määriteltävä ydintoimintaan liittyvät prosessit, ja turvallisuusjohtamisen tehtävänä on tarkastella asioita turvallisuuden näkökulmasta. Leppänen 2006, 24, 72–73.)

Turvallisuusjohtamisen yhtenä määrittävänä tekijänä on turvallisuuskulttuuri. Turvallisuuskulttuurin käsitteen syntyminen tapahtui Tšernobylin ydinonnettomuuden tutkinnan yhteydes-

sä. Tutkinta johti käsitteen turvallisuuskulttuuri syntymiseen ja tämän jälkeen ydinvoimaloiden lisäksi mm. kemianteollisuus ja ilmailuala ovat ryhtyneet tätä käyttämään. (Leppänen 2006, 194.) Yhteiskunnan turvallisuuskulttuuri perustuu kahteen osa-alueeseen: kansallisen käytäntöön turvallisuuden turvallisuuteen liittyvissä asioissa ja ihmisten toimintaan kyseisissä käytännöissä. Kulttuuri muodostuu yrityksen toimintatavoista ja yksittäisen ihmisten asenteesta (Leppänen 2006, 195). Turvallisuutta koskevat asenteet, arvot ja uskomukset muodostavat yhdessä turvallisuustoimenpiteiden kanssa turvallisuuskulttuurin. Turvallisuuteen liittyy myös perusolettamuksia, jotka tarkoittavat riskejä, joihin varaudutaan, vaikka niiden toteutumiseen ei uskota. Tästä voidaan käyttää esimerkkinä valtioon kohdistuvaa aseellista hyökkäyksen uhan olemassaoloa. (Leppänen 2006, 193–194.)

Turvallisuuskulttuuri muodostuu asenteista ja olettamuksista sekä johtamisesta. Asenteet kuvaavat suhtautumistamme riskeihin, sekä miten voimakkaita ja todennäköisiä niiden seuraukset ovat. Työntekijä on vastuussa omista riskeistään ja niiden seurauksista, mutta ryhmään kuuluessamme vastaamme omasta toiminnastamme ja riskeistä myös muille ryhmän jäsenille. Mikäli ryhmän riskikäsitykset ovat samansuuntaiset, ryhmään kuuluvien on mahdollista muokata omia asenteitaan ryhmän käsityksen mukaiseksi. Mikäli ryhmän ja yksilön käsitykset ovat ristiriidassa, vaihtaa yksilö omia asenteitaan tai vaihtaa ryhmää. Asenteet ovat kuitenkin yksilöllisiä, ja kulttuurillisuus on enemmän kuin osiensa summa. (Leppänen 2006, 185 -187.) Jokaisella työntekijällä on oma käsitys turvallisuudesta. Ryhmäpaine kuitenkin ohjaa työntekijöiden omia asenteita ja arvoja.

Kiwa Inspectan (2017) järjestämässä tilaisuudessa kokoontuivat yritysturvallisuuden asiantuntijat pohtimaan, mikä on maailmanluokan turvallisuusjohtamista. Tilaisuuden tavoitteena on kehittää turvallisuusjohtamisen viitekehystä, joka hyödyntäisi yrityksiä koosta tai toimialasta riippumatta. Asiantuntijat määrittelivät turvallisuusjohtamiseen kolme eri tasoa: yksi lakisääteinen taso (Täyttää lainsäädännön ja viranomaisten minimitason) kaksi Sertifiointikelpoinen taso (Täyttää standardien vaatimukset, mahdollistaa sertifioinnin) kolme Maailmanluokan taso (oppiva organisaatio, asettaa itse tavoitteet ja näille indikaattorit, turvallisuus on osa kaikkea johtamista). Yrityksen tulee määritellä taso, joka halutaan saavuttaa. Maailmanluokan taso vaatii resurssointia, ja vain harvat ulkopuoliset tahot huomioivat turvallisuusjohtamisen tason. Turvallisuudesta harvoin uutisoidaan positiivisuuden kautta, jolloin heikko turvallisuustaso on negatiivinen tekijä yrityksen maineelle. Myös maine on yksi riskienhallinnan suojattavista kohteista.

Riskienhallintaa käsitellään standardissa ISO 31000 (2018). Standardi määrittelee riskienhallintaan liittyvät prosessit tarkemmin. Standardin mukaan prosessiin kuuluu toimintaympäristön määritteleminen, periaatteiden, menettelyjen ja käytäntöjen järjestelmällinen viestintä ja tiedonvaihto sekä riskien arviointi, käsittelyyn seurantaa, katselmointi, kirjaaminen ja raportointi. Standardissa 31000 (2018), kuten myös standardi 27001 (2017) ja Leppänen (2006),

määrittelevät että riskienhallinnan prosessien on oltava osa johtamista ja päätöksentekoa. Standardia ei käsitellä tarkemmin osana tietoperustaa.

3.4 Verband der Automobilindustrie information security assessment

Toimialalla on käytössä saksan autoteollisuuden yhdistyksen eli Verband Der Automobilindustrie (Myöhemmin käytetään lyhennettä VDA) tuottama tietoturvallisuuden itsearviointilomake, joka on mahdollista myös sertifioida käyttäen kolmannen osapuolen tekemää auditointia. Arviointi perustuu ISO 27XXX -standardisarjaan, joka on käsitelty osana tietoturvallisuuden hallintajärjestelmä -osioita. Standardin lisäksi arvioinnissa käsitellään toimialakohtaisia määreitä esimerkiksi prototyyppien suojaamiseen liittyen. (VDA 2017.)

Itsearviointilomake on selkeä, koska vaatimukset ovat kysymysmuodossa. Kuvioissa kaksi on kuvatta kohta itsearviointilomakkeesta, jossa määritellään arviointiasteikko ja tarkentavat määreet. Arviointiin käytetään viisiportaista asteikkoa, ja jokaisen kysymyksen arviointiasteikko on kuvattu yksityiskohtaisesti. Tämän lisäksi lomakkeesta löytyy tarkentavat määreet mihin standardin kohtiin viitataan. Kysymysten lisäksi lomakkeesta löytyvät suorituskykymittarit eli Key Performance Indicator, josta käytetään myöhemmin termiä KPi. Kuvioissa kolme on kuvattu esimerkki KPi vaatimuksista. Vaatimuksista löytyvät selkeät määreet mistä aihealueista suorituskykymittari rakentuu, sekä kuinka kauan tietoa tulee säilyttää. (VDA 2018.) Säilytysaikojen määritteleminen itsearviointilomakkeessa helpottaa myös säilytysaikojen määrittelyä tarkasteltaessa vaatimuksia tietosuoja-asetuksen näkökulmasta.

1 General aspects

1.1 **To what extent is an Information Security Management System approved by the organization's management and is its scope documented.**
(Reference to ISO 27001: 4 and 5.1)

Objective:	Systematic control and review of information security within the specified scope is effected by means of the establishment, operation and further development of an Information Security Management System (ISMS) and the assignment of responsibilities. The ISMS must define processes and procedures in order to achieve the information security objectives with respect to adequate confidentiality, availability and integrity of the company assets based on the security policy.
Requirements:	This must include: + The organization's requirements for an ISMS are determined. + An ISMS approved by the organization's management is established. + The scope of the ISMS is specified (e.g. organization in whole or in part). + A Statement of Applicability (SoA) is provided (e.g. filled-in VDA ISA catalogue). This should include: + Criteria (e.g. characteristic values or quantities) for information security assessment are specified. This may include: + Certification in accordance with ISO 27001:2013 (including Scope Statement and SoA). Additionally in case of high protection needs: None. Additionally in case of very high protection needs: None.

Kuvio 1: Kuvankaappaus VDA:n (2018) vaatimuksista

Control	7.2 Awareness and training of employees	
VDA ISA target maturity level	4	
Scope	COVERAGE	EFFEKTIVENESS
ID	**Coverage degree of awareness measures**	**Effectiveness of awareness measures**
Description	Employees with raised awareness represent an important pillar for the information security in a company. Awareness measures should reach all employees, as far as possible. The KPI measures the coverage degree of trainings such as e-learnings, classroom trainings.	The contents of awareness measures should consider outcomes of information security incidents. The KPI measures the effectiveness of awareness measures by collection (number or cost based) of security incidents with human errors as a cause.
Objective (Vision)	All employees are trained with respect to information security	No information security incidents with human error as a cause
Recipient	Information Security; supervisors	Information Security
Frequency (reporting)	to be determined individually (e.g. annually)	to be determined individually (e.g. annually)
Threshold levels	to be determined individually (e.g. Green: > 90%, Yellow: 70-90%, Red: < 70%)	to be determined individually (0-20...low, 20-50 medium, 50+ high) possible characteristic for comparability of business units: in relation to the number of employees e.g. unit: incidents/100 employees
Measurement	Analysis training management Quotient: number of participants/total number of employees	Determining the number of security incidents with human error as a cause
Frequency (measurement)	to be determined individually (e.g. annually)	to be determined individually (e.g. annually)
Interfaces	HR - Training Department - IKS - Internal Audit Department	Incident Management
Components	E-learnings, classroom training, training plan, training register	Incident Mgt. Tool, Ticket System, ISMS Tool
Data archiving	5 years	5 years

Kuvio 2: Kuvankaappaus VDA:n (2018) KPi

Tietoturvallisuustaso on mahdollista auditoida VDA:n mukaisella kriteeristöllä käyttämällä Trusted Information Security Assessment Exchange (myöhemmin käytetään lyhennettä TISAX) -yrityksen hyväksymää ja osoittamaa auditointiyritystä. Käyttämällä TISAX:n hyväksymää yritystä auditoinnissa mahdollistetaan toimialakohtainen tietoturva-auditointi, jota on mahdollista käyttää esimerkiksi sopimusneuvotteluissa. Arviointi on neliosainen koostuen rekisteröinnistä, auditointiyrityksen valinnasta, auditoinnista ja auditointituloksen jakamisesta. (TISAX 2017.) Auditointi voidaan tehdä myös ennen asiakkaan vaatimusta auditoinnille. Tällä toimintatapamallilla yritys voi osoittaa oman tietoturvallisuustasonsa esimerkiksi sopimusneuvotteluissa. Auditoinnin suorittamisen jälkeen yrityksen on mahdollista valita, kenelle annetaan oikeus tarkastella auditoinnin tuloksia.

3.5 Euroopan unionin tietosuoja-asetus

Euroopan unionin tietosuoja-asetuksen tavoitteena on yhtenäistää tietosuojaa koskeva sääntely Euroopan unionin alueella. Yhtenäinen säätely mahdollistaa palveluiden digitalisaation ja luo samalla luottamusta sähköisiin palveluihin. Asetus määrittää myös hallinnolliset sanktiot ja tarkastusoikeudet, minkä avulla voidaan valvoa asetuksen noudattamista. Tämän lisäksi asetusta sovelletaan myös Euroopan unionin alueen ulkopuolella oleviin yrityksiin sekä julkiseen että yksityisen sektoriin riippumatta käsittelyn laajuudesta, luonteesta tai teknologiasta. Asetus on astunut voimaan toukokuun 24. päivänä vuonna 2016, ja siirtymäajaksi on määritelty kaksi vuotta. (Tietosuojavaltuutetun toimisto 2017.)

Tietosuoja-asetus antaa rekisteröidyille aiempaa paremmat edellytykset kontrolloida omia henkilötietojaan ja velvoittaa yrityksiä helpottamaan rekisteröityjen tiedonsaantia sekä varmistamaan henkilötietojen suojaaminen riippumatta siitä, missä henkilötietoja käsitellään. Rekisteröidyt saavat uusia oikeuksia, kuten esimerkiksi oikeuden tulla unohdetuksi, joka tarkoittaa henkilön oikeutta poistaa tietoja rekistereistä sekä tiedottamisvaatimuksen, mikäli henkilötietoihin on kohdistunut tietoturvaloukkaus. Asetus määrittää myös yritykselle sisäänrakennetun ja oletusarvoisen tietosuojan, joka määrittää tietosuojan huomioonottamisen osana palveluiden suunnitteluvaihetta. Rekisteröidyllä tarkoitetaan henkilöä, jonka tietoja on tallennettu henkilötietoja sisältyvään tietojoukkoon, josta tiedot ovat saatavilla tietyin perustein (Tietosuoja-asetus 679/2016, 4§). Yrityksellä on myös osoitusvelvollisuus asetuksen noudattamisesta, ja tietosuojavaltuutetun toimistolla on oikeus tarkistaa yrityksen tietosuojaan liittyviä prosesseja ja käytänteitä. (EU yleinen tietosuoja-asetus 679/2016.)

Osana osoitusvelvollisuutta sekä sisäänrakennettua ja oletusarvoista tietosuojaa yrityksen pitää pystyä todentamaan, miten käyttäjät on koulutettu tietosuojaan ja tietoturvallisuuteen. Sisäänrakennettu tietosuoja edellyttää, että tietosuojaperiaatteet on otettu tehokkaasti käyttöön kaikissa henkilötietojen käsittelyn vaiheissa (Tietosuojavaltuutetun toimisto 2017). Järjestelmien tekninen suojaaminen on mahdollista varmistaa määrittelyillä sekä rakentamalla järjestelmä asetuksen mukaiseen kuntoon esimerkiksi ottamalla lokitietojen kirjaaminen ja valvonta osaksi toimintaa käsiteltäessä henkilötietoja.

Tietosuoja-asetuksen (679/2916) 32§ neljäs kohta määrittelee, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita. Artikla määrittää, että henkilötietojen käsittelijällä tulee olla ohjeet, miten henkilötietoja käsitellään sekä yrityksen tulee osoittaa, miten työntekijät on koulutettu käsittelemään henkilötietoja. Henkilötietojen käsittelijöitä on eri tehtävissä, ja eri tehtävissä käsitellään eri määriä henkilötieto-

ja. Tämä asettaa yritykselle velvollisuuden tarkastella, miten eri henkilöryhmät koulutetaan ja ohjeistetaan käsittelemään henkilötietoja. (EU yleinen tietosuoja-asetus 679/2016.)

Asetus määrittää, että henkilötietoja olisi käsiteltävä siten, että varmistetaan henkilötietojen asianmukainen turvallisuus ja luottamuksellisuus, millä muun muassa ehkäistään luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin laitteistoiin sekä tällaisten tietojen tai laitteistojen luvaton käyttö. Tulevaisuudessa valvontaviranomaisen antamat ohjeistukset, hallinnolliset päätökset ja sanktiot määrittelevät tarkemmin asetuksen hengen. Asetuksen asettamiin hallinnollisiin päätöksiin ja sanktioihin vaikuttavat myös voimassa olevat käytännöt tietosuojasta ja tietoturvallisuudesta. (EU yleinen tietosuoja-asetus 679/2016, 5§.)

Hallituksen esityksessä (Eduskunta 2018) ehdotetaan, että Suomessa otetaan käyttöön tietosuoja-asetusta täydentävä tietosuojalaki. Lain tehtävänä on täydentää ja täsmentää tietosuoja-asetusta ja laki ei muodostaisi itsenäistä ja laajaa sääntelykokonaisuutta, vaan kansallista tietosuojalakia sovellettaisiin rinnakkain tietosuoja-asetuksen kanssa. Kansallisessa laissa säädettäisiin käsittelyn oikeusperustasta, valvontaviranomaisesta, oikeusturvasta, sekä tietojenkäsittelyn erityistilanteista. Asetuksessa on yrityksen näkökulmasta vielä paljon avoimia kysymyksiä, jotka selviävät vasta kansallisen tietosuojalain voimaantulon ja oikeuskäytännön jälkeen. Perusajatuksena yrityksen näkökulmasta on ymmärrettävä, missä henkilötietoja säilytetään ja miten niitä käsitellään, sekä mikä henkilötieto on rekisteröidyn kannalta kriittistä, jotta tietoa voidaan suojata tiedon suojaustarpeen mukaan.

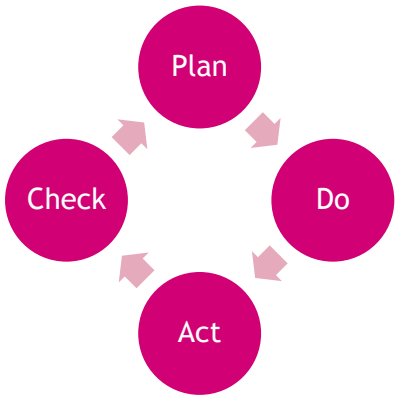
3.6 Laadunhallintajärjestelmä

Laadunhallintajärjestelmän tavoitteena on vastata toimintaympäristön asettamiin haasteisiin ja täyttää asiakkaiden asettamia vaatimuksia sekä pyrkiä ylittämään asetetut tavoitteet. Yritysten toimintaympäristö on hyvin erilainen kuin viime vuosikymmeninä. Kiihtyvä muutos, markkinoiden kansainväistyminen sekä osaamisen nouseminen tärkeäksi resurssiksi kuvaavat kiihtyvää muutosta. Laatu on tekijä, joka vaikuttaa asiakastyytyväisyyteen, ja sillä voi olla myös vaikutusta yrityksen maineeseen, mikäli tuotteen laatu ei ole odotuksen mukainen. (ISO 9000 2015.)

Laadunhallintajärjestelmän tehtävänä on kattaa kaikki yrityksen toiminnot, joilla yritys määrittää tavoitteet, prosessit ja resurssit, joilla saavutetaan yrityksen halutut tulokset. Järjestelmässä määritellään resurssit ja prosessit, joilla saavutetaan arvon ja tulosten tuottaminen olennaisille sidosryhmille. Standardissa määritellään, että ihmiset ovat yrityksen kannalta voimavaroja, joiden toiminta vaikuttaa yrityksen suorituskykyyn. Työntekijät toimivat saman päämäärän eteen, kun heillä on yrityksen johdon kanssa sama näkemys laatupolitiikasta ja halutuista tuloksista. Laadunhallintajärjestelmä on toimiva, kun työntekijät ymmärtävät ja soveltavat taitojaan, koulutustaan ja kokemuksiaan, joita he käyttävät työtehtäviensä hoitamiseen. Ylimmän johdon tulee tarjota työntekijöille mahdollisuus kehittää tarvittavaa osaa-

mista. Parantaminen mahdollistaa yrityksen suorituskyvyn mukaisen tason sekä reagoinnin sisäisiin ja ulkoisten olosuhteiden muutoksiin. Lisäksi se mahdollistaa yrityksen toimintakyvyn ja asiakastyytyväisyyden parantamisen sekä opittujen asioiden hyödyntämisen parannusten tekemisessä. (ISO 9000 2015.)

Laadunhallintajärjestelmä on prosessimainen toimintamalli, joka tehostaa hallintajärjestelmän vaikuttavuutta sekä toteutumista, jotta asiakastyytyväisyys paranee. Prosesseissa tulee ymmärtää, että prosessit ovat osa kokonaisuutta ja yksittäisiä prosesseja tarkasteltaessa tulee tarkastella myös kokonaisprosessin toimintaa. Kokonaiskuvan hallintaan voidaan käyttää Plan, Do, Check, Act-mallia (Suunnittele, toteuta, arvioi, toimi) ja noudattaa toiminnassa riskiperusteista lähestymistä. (ISO 9000 2015.) Malli on avattu tarkemmin kuvioissa kolme.



Kuvio 3: Plan, Do, Act, Check malli (ISO 9000 2015.)

Riskiperusteisen toiminnan tavoitteena on mahdollisuuksien hyödyntäminen ja ei-toivuttujen tulosten estäminen. Suunnittelussa asetetaan tavoitteet prosesseille ja järjestelmille sekä määritellään resurssit, joilla tavoitteet voidaan saavuttaa. Suunnittelussa huomioidaan myös riskit ja mahdollisuudet. Toteuta -vaiheessa toteutetaan suunnitelma. Arviointivaiheen tavoitteena on mitata tuotteita ja palveluita sekä verrata niitä tavoitteisiin ja vaatimuksin. Arviointivaiheen tuloksista raportoidaan päätöksenteon tuoksi. Toimi vaiheessa -raportoinnin perusteella kehitetään järjestelmän suorituskykyä. (ISO 9000, 2015.)

Riskiperusteinen toimintamalli on olennainen osa laadunhallintajärjestelmän toteuttamista. Toimintamallin perustana on ennaltaehkäistä mahdollisia poikkeamia, toteuttaa poikkeamien analysointia ja estää poikkeamien toistuminen tarkoituksenmukaisella tavalla poikkeamien vaikutuksiin nähden. Riskiperusteisessa toiminnassa on myös tarkasteltava mahdollisuuksia, joita uudet prosessit antavat omalle toiminnalle ja asiakkaille. (ISO 9000 2015.)

Päätöksenteko perustuu käytössä olevan datan ja informaation analysointiin. Päätöksentekoon perustuu aina epävarmuutta, ja prosessit voivat olla monimutkaisia. Syy-seuraussuhde sekä mahdolliset tahattomat seuraukset tulee ymmärtää osana päätöksentekoa. Perustuessaan

tosiasioihin ja käytettävissä olevaan analysointiin päätökset johtavat parempaan luotettavuuteen. Toimintatapamallilla saavutetaan prosessien suorituskyvyn kasvamista ja tavoitteiden helpompaa arviointia. (ISO 9000 2015.)

Johdonmukaiset ja ennustettavat tulokset voidaan saavuttaa tehokkaammin ja vaikuttavammin, kun johdetaan kokonaisuutta ja toisiinsa liitettyjä prosesseja. Yrityksen tulee ymmärtää, miten kokonaisuus ja prosessit toimivat. Näin voidaan tuottaa parempia tuloksia ja optimoida järjestelmän suorituskykyä. Tunnistamalla kokonaisuus ja tärkeimmät prosessit voidaan kehittämiseen käytettävät voimavarat kohdentaa oikeisiin järjestelmiin ja prosesseihin. (ISO 9000 2015.)

Yrityksen tehokkaan toiminnan kannalta työntekijöiden tulee tuntea itsensä osaksi kokonaisuutta ja tietää oma roolinsa isossa kokonaisuudessa. Mikäli työntekijät ymmärtävät organisaation tavoitteet ja oman roolinsa, he ovat tyytyväisempiä työhönsä, ja heillä on motivaatiota saavuttaa asetetut tavoitteet. Samalla myös yrityksen luottamus kehittyy ja yhteistyö lisääntyy. Työntekijöille tulee viestiä aktiivisesti, jotta he ymmärtävät oman työnsä tärkeyden. Tehdylle työlle tulee myös antaa tunnustusta. (ISO 9000 2015.)

4 Tutkimusasetelma ja -menetelmät

Opinnäytetyö perustuu yrityksen tavoitteeseen kehittää käyttäjien tietoturvallisuustietoisuutta ja koulutusta vastaamaan nykytilanteen vaatimuksia. Opinnäytetyö aloitettiin määrittelemällä tutkimuskysymykset, joilla vastataan yrityksen tavoitteisiin. Tämän jälkeen määriteltiin opinnäytetyön tutkimusstrategia sekä valittiin menetelmät työn toteuttamiseen.

Tutkimusstrategiaksi valittiin tapaustutkimus, koska tavoitteena on selvittää yksittäinen tapaus, tilanne tai joukko tapauksia (Hirsjärvi, Remes & Sajavaara 2006, 130–131.) ja tuottaa ideoita ja kehitysehdotuksia. Tapaustutkimus on yksi laadullisen eli kvalitatiivisen tutkimuksen lajeista. Hirsijärvi, Remes ja Sajavaara (2006, 157) määrittelevät laadullisen tutkimuksen tavoitteeksi todellisen elämän kuvaamisen mahdollisimman kokonaisvaltaisesti. Tapaustutkimus on kartoittava tutkimus, jonka tavoitteena on selvittää tietoturvallisuuteen liittyvien ohjeiden nykytilanne ja määritellä kehitysehdotukset niiden parantamiseksi. Tapaustutkimuksen avulla voidaan ymmärtää kehittämiskohdetta kokonaisvaltaisesti. Opinnäytetyössä tutkittava kohde on valittu työelämän käytännön tarpeen ja tavoitteiden ohjaamana. (Ojasalo, Moilanen, Ritalahti 2014, 52–53.) Jyväskylän yliopisto (2015) määrittelee, että tapaustutkimukseen ei ole määritelty, mitä menetelmiä käytetään.

Tutkimuksen menetelmäksi valittiin dokumenttianalyysi. Menetelmä valinnan perustana ovat tutkimuskysymykset sekä toimeksiantajan tavoite analysoida voimassa olevia ohjeistuksia ja verrata niitä nykytilanteeseen. Menetelmä valinnan perustana on myös tavoite tehdä kirjalliseen muotoon tehdyistä aineistosta päätelmiä. Ojasalo, Moilanen ja Ritalahti määrittelevät,

että tarkastelun kohteena olevat dokumentit voivat olla raportteja, WWW-sivuja, keskusteluja ja muuta kirjallista materiaalia. Menetelmän tavoitteena on analysoida yrityksen tuottamia dokumentteja ja luoda järjestelmällisesti selkeä kuvaus tutkittavasta ja kehitettävästä aiheesta. Analyysin vahvuudeksi Ojasalo, Moilanen ja Ritalahti määrittelevät, millaisena kehittämiskohteena oleva ilmiö on luonnollisessa ympäristössä. Tarkastelun kohteena on yrityksen sisäinen dokumentaatio asiakirjanhallintajärjestelmästä ja saatavilla oleva koulutusmateriaali. Materiaaliin tulee suhtautua kriittisesti, koska materiaali on voitu tuottaa eri vaatimuksia tarkasteltaessa. (Ojasalo, Moilanen, Ritalahti 2014, 43, 54–57, 130, 136.)

Menetelmäoppaan (Ojasalo, Moilanen, Ritalahti 2014, 110) mukaan laadullisella analyysillä kerätty tieto analysoidaan useaan kertaan, ja näin määritellään yhtymäkohdat viitekehyksen teoriaan. Analyysi on jaettu kolmeen eri vaiheeseen: Yksi mahdollisimman laaja-alaisesti dokumentaation kerääminen, kaksi materiaalin analysointi ja pelkistäminen sekä kolme analysoidun materiaalin tulkinta ja johtopäätökset. (Ojasalo, Moilanen, Ritalahti 2014, 131–144.)

Ensimmäisessä vaiheessa tieto kerättiin yrityksen eri tietovarainnoista. Ensisijainen tietolähde oli asiakirjanhallintajärjestelmä, josta yrityksessä löytyy tarkastettu ja hyväksytty dokumentaatio. Toissijainen tietolähde oli yrityksen verkkolevyt ja muut vastaavat dokumentteja käsittelevät järjestelmät. Toisessa vaiheessa tietoa kerättiin työntekijöiltä. Toinen vaihe oli kriittinen, koska esimerkiksi sopimukset ja niiden liitteet kuvaavat tarkemmin asetetut vaatimukset yritystä kohtaan. Kaksivaiheiselle toiminnalle pystyttiin erottamaan vaatimukset ja voimassa olevat ohjeet sekä koulutusmateriaalit toisistaan. Toimintamalli helpotti seuraavia työn vaiheita.

Toisessa vaiheessa tieto analysoitiin ja pelkistettiin jakamalla kerätty materiaali kahteen osa-alueeseen vaatimukset ja voimassa olevat ohjeet. Materiaalin jakaminen tukee vaiheen kolme suorittamista, koska toiminannalla saadaan selkeästi jaettua materiaali omiin osa-alueisiinsa ja materiaalin käsitteleminen on yksinkertaisempaa. Kerätty materiaali pelkistettiin poistamalla selkeästi vanhentunut materiaali sekä materiaali joka ei ole työn tekemisen kannalta relevanttia.

Materiaalin analysoinnin tueksi luotiin kolme taulukkoa, jotka ovat kuvattu tarkemmin nykytila-analyysi kappaleessa. Liitteet toimivat tulkintojen ja johtopäätöksien perustana. Materiaalin käsittelyyn valittiin ohjaavaksi viitekehykseksi ISO 27001 (2017) standardi, koska viitekehyksenä ja opinnäytetyön tavoitteiden kannalta valinta tuki työn tekemistä. Käsittelyyn helpottamiseksi osa-alueet jaettiin kolmeen dokumenttiin, josta tuotettiin liitteet käsittelyn helpottamiseksi.

5 Nykytila-analyysi

Ensimmäisenä tarkastellaan nykytila-analyysin tuloksia, jonka jälkeen käsitellään kohdat ylimmän johdon ohjaus sekä käyttäjän ohjeet. Nykytila-analyysi vastaa ensimmäiseen tutkimuskysymykseen: mikä on tietoturvallisuusohjeiden nykytilanne. Käyttäjän ohjeet vastaa toiseen tutkimuskysymykseen: Mitä tietoturvaohjeita käyttäjät tarvitsevat ja miksi. Nykytilanteen kuvaaminen ja tilanteen vertaaminen vaatimuksiin määrittelevät kehityskohteet. Nykytila-analyysissä on tärkeä huomioida, että dokumentaatio on rakennettu eri viitekehykseen verrattaessa. Osion rakenne noudattelee ISO 27001 (2017) rakennetta, koska tällä tavalla lukijan on helpompaa seurata tuloksia ja verrata analyysin kohtia vaatimuksiin sekä seurata ja löytää tarvittava tietoa liitteistä.

Opinnäytetyötä ja nykytila-analyysiä varten tehtiin kolme liitettä. Liite yksi yritystä koskevat vaatimukset ISO 27001 (2017) viitekehyksenä vertaa standardin, tietosuoja-asetuksen ja VDA:n vaatimusten keskeiset suhteet. Liite antaa kokonaiskuvan, miten vaatimukset ovat verrattavissa toisiinsa nähden. Viitekehykseksi valittiin standardi, koska se on ollut pisimpään käytössä sekä rakenne on selkeä ja johdonmukaisin vaatimuksista. Tietosuoja-asetuksen sarake on otettu materiaali julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) järjestämästä tietosuojayhteishankkeen materiaalista (Valtionvarainministeriö 2018). VDA sarake on kerätty itsearviointilomakkeesta ja verrattavat kohdat on poimittu viitekehyksen mukaisesti. Lomakkeessa käsitellään myös paljon muitakin vaatimuksia, mutta aihealueen rajaus on rajannut kohdat pois esimerkiksi teknisen tietoturvallisuuden toteuttamisen osalta. Liite antaa lukijalle kokonaiskuvan vaatimusten suhteista. Standardia käytetään työn viitekehyksenä, koska standardin rakenne kuvaa johdonmukaisesti tietoturvallisuuden hallinnan vaatimuksia. Nykytila-analyysissä ei käsitellä kokonaisuudessaan standardia, tietosuoja-asetusta ja VDA kriteeristöä, koska opinnäytetyö käsittää käyttäjää koskevia ohjeita.

Liitteeseen kaksi kerättiin voimassa olevat ohjeet sekä koulutusmateriaali. Liitteessä kolme verrattiin voimassa olevia vaatimuksia liitteen yksi perusteella ja liitteeseen kaksi kerättyjä ohjeita sekä koulutusmateriaalia. Voimassa olevat ohjeet ja koulutusmateriaali kerättiin yrityksen tietovarannoista. Materiaalin kerääminen ensin omilta osa-alueiltaan omiksi liitteiksi ja niiden yhdistäminen liitteeseen kolme helpotti työn tekemistä ja osa-alueiden selkeyttämistä omiksi kokonaisuuksiksi.

Nykytila-analyysin tuloksena pystyimme määrittelemään mitä osa-alueita voimassa olevat ohjeistukset täyttävät ja missä osa-alueissa on puutteita. Tärkeimpänä havaintona on kuitenkin materiaalin haasteellinen saatavuus ja ohjeistuksen yleisluonteisuus. Vaatimusten kerääminen sidosryhmiltä ja sopimuksista oli helppoa, koska materiaalilla on selkeät omistajat ja tieto on yksinkertaisintoimin saatavilla järjestelmistä. Voimassa olevien ohjeiden ja koulu-

tusmateriaalin kerääminen oli haasteellista, koska materiaali on pirstoutunut eri järjestelmiin ja kansioihin.

5.1 Ylimmän johdon ohjaus

Ylimmän johdon ohjaus käsittää toimintaympäristön määrittelemisen ja tiedottamisen sekä politiikkojen päivittämisen ja noudattamisen sekä valvonnan. Johdon tulee päivittäisessä toiminnassaan opastaa ja ohjata omia alaisiaan. Toiminta vaikuttaa merkittävästi turvallisuuskulttuurin ylläpitämiseen ja kehittämiseen.

Ylin johto ohjaa sopimuksista ja muista ulkoisista tekijöistä tulevien toimintaympäristöön vaikuttavien vaatimusten tiedottamisessa ja selvittämisessä. Ylimmän johdon tärkein tehtävä on jakaa sidosryhmien tarpeita ja vaatimuksia vastuuyksiköille. IT- ja HSE-osasto tukevat toimintaa käsittelemällä sidosryhmien vaatimukset ja odotukset, sekä vertaavat uusia vaatimuksia voimassa oleviin toimintatapoihin. Toimintaympäristön määritteleminen on strategian tukemisen kannalta kriittinen osa-alue. (ISO 27001, 2017.) Opinnäytetyö on osa toimintaympäristön määrittelyä, koska opinnäytetyöhön on koottu asiakasvaatimukset tietoturvallisuuteen liittyen.

Tietoturvallisuuspolitiikka on ylimmän johdon pysyvä tahtotila tietoturvallisuuden toteuttamiseen. Tietoturvapolitiikan tehtävänä on varmistaa riittävät resurssit, tukitoiminnat, toiminnat tietoturvallisuuden toteuttamiseen sekä määritellä suorituskyvyn arviointiin, parantamiseen, johtajuuteen ja tietoturvallisuuden katselmointiin liittyvät tavoitteet. Käyttäjän näkökulmasta tietoturvapolitiikka on ylimmän johdon julkilausuma tietoturvallisuustyöstä, ja se määrittää myös käyttäjälle vaatimuksia. Politiikka on ylätason asiakirja, joka määrittää periaatteet tietoturvallisuuteen. Periaatteet määrittävät esimerkiksi, että tiedon on oltava riittävän suojassa. Käyttäjälle suunnatut ohjeet määrittävät, mitkä ovat käyttäjän toimenpiteet, jotta tieto pidetään riittävän suojassa. Suojaus perustuu riskienhallintaan ja asiakasvaatimuksiin. Politiikka ei ota kantaa teon rangaistavuuteen, mutta määrittää, että poikkeamat tutkitaan, jotta vastaavaa poikkeamaa ei enää tulevaisuudessa tapahtuisi. (ISO 27000 2017, VDA 2018, EU yleinen tietosuoja-asetus 679/2016.)

Riskienhallinnassa noudatetaan yrityksen riskienhallintapolitiikkaa. Politiikassa määritellään riskienhallintaan liittyvät käsitteet ja vastuut. Riskienhallinnan suorittamisella mahdollistetaan tietoturvallisuuteen liittyvien toimenpiteiden kohdentaminen sekä tietoturvallisuuden vaikuttavuuden arviointi. (ISO 27001 2017; VDA 2018; EU yleinen tietosuoja-asetus 679/2016.)

Ylimmän johdon ohjaus on yrityksessä hoidettu tietoturva- ja riskienhallintapolitiikalla, jotka määrittävät ylätason toiminnan ja tavoitteet sekä muut ohjaavat määreet. Tietoturvapolitiikan jalkauttaminen yrityksen toiminnan osaksi on puutteellinen. Politiikka on julkaistu asiakirjanhallintajärjestelmässä, mutta muuten politiikasta ei ole viestitty työntekijöille. Voimas-

sa olevassa ohjeistuksessa ei myöskään käsitellä politiikan näkökulmasta. Riskienhallintapolitiikka on viestitty työntekijöille ja se ohjaa paremmin, tietoturvapolitiikkaan verrattuna, yrityksen toimintaa. Riskienhallinnan haasteena on, että politiikan alapuolella oleva tietoturvallisuuden ohjaus puuttuu. Ohjauksen tavoitteena olisi tarkemmin määritellä politiikan toiminta tietoturvallisuudessa asettamalla raja-arvoja ja määreitä tietoturvallisuuden riskienhallinnan toteuttamiseen.

5.2 Käyttäjän ohjeet

Voimassa olevat käyttäjäohjeet ja koulutusmateriaali on kuvattu ja jäsennelty liitteessä kaksi. Liite on poistettu salassapitosyistä opinnäytetyön julkaistavasta versioista. Liite sisältää ja kuvaa yrityksen tietoturvallisuuden organisoimisen, mobiililaitteet ja etätyön, henkilöstöturvallisuuden, vastuut, pääsynhallinnan fyysisen turvallisuuden, käyttöturvallisuuden, vaatimuksenmukaisuuden sekä tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinnataan liittyvien ohjeiden nykytilanteen. Lisäksi liitteessä aluksi avataan koulutusprosessia tietoturvallisuudesta ja turvallisuudesta sekä kuvataan voimassa oleva koulutusmateriaali. Turvallisuuden kouluttamisen ymmärtäminen tukee lukijan ymmärrystä tarkastella nykytilannetta. Rakenne perustuu ISO 27001:2017 standardiin.

Käyttäjän tulee tietää yrityksen tietoturvallisuuden organisointi, jotta käyttäjä pystyy ilmoittamaan havainnoistaan ja poikkeamista oikealle toimijalle. Politiikassa on eritelty käyttäjän ja esimiehen vastuut tietoturvallisuudessa. Organisointi on kuvattu politiikassa ja yrityksen organisaatiokaavioissa. Politiikka on ohjeistus, johon jokaisen esimiehen tulee tutustua ja joka tulee jalkauttaa omille alaisille ja jonka toteutumista tulee valvoa osana esimiestyötä. (ISO 27001 2017, A6.1.)

Mobiililaitteiden ja etätyöhön liittyvän ohjeistuksen tavoitteena on varmistaa käytön turvallisuus. Tämän lisäksi jokaiselle käyttäjälle luovutetaan mobiililaitteisiin liittyvä ohjeistus, kun käyttäjä noutaa laitteen. Ohjeistuksessa käsitellään pääpiirteisesti mobiililaitteiden käyttämiseen liittyviä tietoturvallisuusnäkökohtia ja käytännön kannalta tarpeellisia asioita kuten esimerkiksi, miten toimitaan, jos laite rikkoutuu tai miten laitetta saa käyttää. Mobiililaitteisiin liittyviä ohjeita löytyy koulutusmateriaalista, mutta selkeä yksittäinen käyttäjäohje mobiililaitteiden käyttämiseen puuttuu. Etätyöohjeen osalta toiminta on samantyyppinen ja -tasoinen. Yrityksen toimintapolitiikan mukaisesti jokaisella etätyöoikeuden omaavalla henkilöllä tulee olla etätyösopimus, jossa käsitellään pääpiirteisellä tasolla etätyöhön liittyviä tietoturvallisuusnäkökohtia sekä käytännön toimintaan liittyviä kohtia. Asiakirjojen suojausluokituksessa otetaan kantaa siihen, missä tiloissa saa käsitellä turvallisuusluokituksen mukaista tietoa, kuten VDA:n vaatimuksissa määritellään. (ISO 27001 2017, A6.2; VDA 2018.)

Henkilöstöturvallisuus on jaettu kolmeen eri osa-alueeseen: ennen työsuhteen alkua, työsuhteen aikana ja työsuhteen päätyttyä tai muututtua. Jokaisen osa-alueen tavoitteena on var-

mistaa työntekijän tai vuokratyöntekijän tietoisuus häntä koskevista tietoturvallisuuden vaatimuksista sekä mahdollistaa turvallinen ja oikea toiminta. Työsopimuksessa käsitellään ylätasolla voimassa olevien ohjeiden noudattamista, ja sopimusta allekirjoittaessa työntekijä allekirjoittaa myös salassapitosopimuksen. Työsuhteen aikana käyttäjää tulee kouluttaa tietoturvallisuuteen liittyen, ja ohjeiden tulee olla käyttäjän saatavilla. Koulutus on VDA:n vaatimuksista tuleva mittari. Mittarin raja-arvona on, että 90 % henkilöstöstä on saanut koulutuksen viimeisen vuoden aikana. Mittari mahdollistaa myös ylimmän johdon tietoturvallisuuden vaikuttavuuden seurannan. Työsuhteen päättymiseen on määritelty prosessi. (VDA 2018; ISO 27001 2017, A7.)

Käyttäjän vastuut suojattavan omaisuuden hallinnassa on määritelty ohjeessa, joka käsittelee IT-järjestelmien loppukäyttäjän toimintaa. Ohjeistus kuvaa käyttäjän IT-järjestelmien käyttämiseen liittyvät turvallisuusnäkökohdat käyttäjän vastuista, suojattavan omaisuuden hallinnasta ja suojattavan omaisuuden vastuut sekä tietovälineiden käsittelystä. Ohjeen lisäksi on käytössä asiakirjojen turvallisuusluokitteluun liittyvä ohjeistus, joka määrittelee, miten tietoa tulee käsitellä. Käsittely kattaa tiedon käsittelyn ja siirron tiedon eri muodoissa. (ISO 27001 2017, A.8.)

Pääsynhallinta jakautuu neljään eri osa-alueeseen: liiketoiminnalliset vaatimukset, oikeuksien hallinta, käyttäjien vastuut ja järjestelmien ja sovellusten pääsynhallinta. Liiketoiminnalliset vaatimukset pääsynhallinnassa on toteutettu käyttämällä keskistettyä ohjelmistoa käyttäjäoikeuksien myöntämisessä ja valvonnassa. Ohjelmisto muodostaa lokitietoa, koska oikeutta on haettu, kuka on hakenut, kuka on tarkistanut oikeuden ja kuka on hyväksynyt, että oikeus voidaan myöntää. Prosessin mukaisesti toimittaessa ei tulisi olla mahdollista, että käyttäjä saisi oikeuksia, mitkä eivät hänelle kuulu. Järjestelmän käyttäminen mahdollistaa myös toiminnan auditoinnin. Käyttäjille on luotu ohjeet, miten järjestelmää käytetään ja miten pääsyoikeuksia hallitaan sekä miten tunnistautumistietoja suojataan ja käytetään. (ISO 27001 2017, A9; VDA 2018, 9.)

Fyysisen turvallisuuden toteuttaminen on ohjeistettu toimintajärjestelmässä olevassa ohjeessa. Ohje määrittää, miten fyysisen turvallisuuden keinoin estetään tunkeutuminen yrityksen tietoaineisoihin ja -palveluihin. Kulunvalvonnassa olevassa ohjeessa määritellään, mitkä ovat käyttäjän vastuut kulunvalvonnassa ja miten käyttäjät toimivat, mikäli he huomaavat kulunvalvonnassa poikkeamia. Ohjeistuksen lisäksi kaikki henkilöt, joilla on pääsy yrityksen tiloihin, käyvät turvallisuuskoulutuksen, jossa tietoturvallisuus on yhtenä osa-alueena. Käyttäjille on olemassa myös ohjeistus, joka kattaa laitteiden turvallisen poistamisen ja kierrättämisen. (ISO 27001 2017, A11; VDA, 2018, 11.)

Käyttöturvallisuuden osa-alueesta käsitellään toimintaohjeet ja -velvollisuudet, jotka on dokumentoitu osana IT-loppukäyttäjän ohjetta sekä osana asiakirjojen suojausluokitusta. Ohjeil-

la varmistetaan, että käyttäjät ovat tietoisia, mitä käyttöturvallisuus heidän toiminnassaan tarkoittaa. Esimerkiksi ohjeissa käsitellään, missä tiedostoja pitää säilyttää, jotta ne kuuluvat yrityksen varmuuskopioinnin piiriin sekä miksi ja koska ohjelmistopäivitykset tulee asentaa. (ISO 27001 2017, A12; VDA 2018, 12.)

Viestintäturvallisuus käsitellään osana loppukäyttäjän ohjetta sekä asiakirjojen suojausluokitusta. Käyttäjän tulee olla tietoinen siitä, mitä tietoa saadaan siirtää verkon eri osissa ja minkälaisessa muodossa tiedon siirtäminen on sallittua. Etätyössä käyttäjä on haavoittuvainen ulkopuolelta tulevaan uhkaan, koska silloin verkon turvallisuus ei ole täysin yrityksen hallinnassa. (ISO 27001 2017, A13; VDA 2018, 13.)

Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinnassa käyttäjän vastuulla on poikkeamien raportointi ja oikeaoppiset toimintatavat. Tavoitteena on varmistaa, että toiminta on johdonmukaista ja vaikuttavaa sekä että tietoturvatapahtumista ja -heikkouksista viestitään tehokkaasti. Koulutuksessa käyttäjät koulutetaan toimimaan yrityksen toimintapolitiikan mukaisesti ja viestimään poikkeamista ja havainnoista prosessien mukaisesti. Yksiselitteinen ja erillinen ohjeistus tietoturvapoikkeamien viestinnästä puuttuu. Politiikka määrittää tietoturvallisuuden häiriöistä viestinnän perusteet ja määrittää käyttäjän vastuulle ilmoituksen tekemisen. (ISO 27001 2017, A16; VDA 2018, 16.)

Vaatimuksenmukaisuus voidaan jakaa kahteen osa-alueeseen: lainsäädännön vaatimukset ja sopimuksiin sisältyvät vaatimukset sekä tietoturvallisuuden katselmointi. Lainsäädännön vaikutukset ovat osa tietosuoja-asetuksen osoitusvelvollisuutta. Yrityksen on todistettava vaatimuksenmukaisuutensa asetukseen. Käyttäjän näkökulmasta tietoturvallisuus ja – suojan koulutus on osa vaatimuksenmukaisuutta. Asetuksen vaatimusten täyttämisen osalta työ on vielä kesken, mutta pääpiirteet ja toimintatavat ovat yrityksellä selkeästi määritelty osaksi prosesseja. Tietosuojapolitiikka määrittää käyttäjän velvollisuudet ja vastuut. (ISO 27001 2017, A18; VDA 2018, 18; EU yleinen tietosuoja-asetus 679/2016.)

Koulutuksen osalta yrityksessä on käytössä prosessi, jossa kaikki käyttäjät koulutetaan turvallisuusperehdytyksessä turvallisuuteen. Koulutuksen yhtenä osa-alueena on tietoturvallisuus ja –suoja. Tämän lisäksi esimiehelle kuuluu perehdytysprosessissa tietoturvallisuuden kouluttaminen. Perehdytysprosessista jää dokumenttijälki työntekijän tiedostoihin, jolla täytetään osittain standardin ISO 27001 (2017) kohta A.7.2.2 sekä VDA (2018) kohta 7.2 ja todennetaan KPi:t, jonka vaatimuksena on kaikkien työntekijöiden koulutuksesta.

6 Johtopäätökset ja kehitysehdotukset

Nykytila-analyysia varten tehdyt liitteet toimivat opinnäytetyön johtopäätösten ja kehitysehdotusten pohjana. Osa johtopäätöksistä ja kehitysehdotuksista käsitellään tässä osiossa. Osa ehdotuksista ja havainnoista käsitellään osana yritykselle tehtävää erillistä esittelyä. Opin-

näytetyö vastasi tutkimuskysymykseen turvallisuusohjeiden nykytilasta osioissa nykytila-analyysi, jossa kuvattiin nykytilanne tietoturvaohjeissa. Osioissa käyttäjän ohjeet vastattiin mitä ja miksi käyttäjät tarvitsevat tietoturvaohjeita.

Turvallisuusohjeet ovat osa turvallisuuskulttuuria ja kulttuurin kehittämistä. Ajantasainen ohjeisto ja käytännön toimintaan liittyvät esimerkit kuvaavat käyttäjälle sen, miksi tietoturvallisuustyö on tärkeää. Käytännön esimerkit konkretisoivat ohjeistuksen yrityksen ympäristöön sekä tuovat ohjeet osaksi työntekijän arkea. Suunnittele, toteuta, arvio ja toimi -mallin mukaisesti käyttäjälle kuuluvat ohjeet tulee tarkastaa myös käyttäjien näkökulmasta erikseen määritellyin väliajoin. Tietoturvallisuusohjeita kirjoittavien substanssi käsiteltävään aiheeseen voi aiheuttaa käyttäjälle haasteita ohjeiden ymmärtämisessä.

Turvallisuusjohtamisen näkökulmasta on hyvä myös huomioida, että vaikka vaatimukset määrittelevät ja ohjaavat toimintaa sekä suorituskykymittareita, ei toiminnan tavoitteena tule olla pelkästään vaatimusten täyttäminen. Toiminnan pitää tukea yrityksen strategiaa, ja turvallisuustoiminnan tehtävänä on varmistaa ja mahdollistaa ydinprosessin toteutuminen kaikissa tilanteissa. Vain tavoitteiden saavuttamiseen sekä varmistamiseen tähtäävä toiminta on tärkeää (Leppänen 2014).

Yrityksessä on käynnistetty turvallisuusohjeiden ja hallintajärjestelmän kehittäminen työn aikana esiin tulleiden kehityskohtien perusteella. Tutkijan näkökulmasta yrityksen toimintatavoissa on kehitettävää, mutta opinnäytetyöhön on sitouduttu ylimmän johdon toimesta positiivisesti ja kehityskohteiden esittäminen on nostanut ylimmän johdon tietoturvatietoisuutta ja käsitystä siitä, miksi tietoturvallisuus ei ole vain pakollinen paha yrityksen toiminnassa vaan lisäksi merkittävä kilpailutekijä kiristyvillä markkinoilla.

Tärkeimpänä kehitysehdotuksena on ohjeiden saatavuuden parantaminen. Dokumenttianalyysiä tehtäessä materiaalin kerääminen eri tietojärjestelmistä oli haastavaa. Mikäli käyttäjän tarvitsema materiaali on käyttäjän helposti saatavilla, käyttäjä pystyy tarkistamaan hänelle asetetut vaatimukset sekä toimimaan ohjeistuksen mukaan. Kehitysehdotus perustuu standardi 27001 (2017) kohtiin 7.2 & 7.3 ja VDA:n (2018) kohtiin 7.1 & 7.2. Vaatimukset käsittelevät henkilöstön pätevyyttä ja tietoisuutta suorittaa omat työtehtävänsä turvallisesti. Tällä hetkellä käytössä ei ole esimerkiksi sisäisellä kotisivulla selkeää paikkaa, mihin turvallisuuden eri osa-alueen tiedostot olisi kerätty loogiseen ja helposti sekä nopeasti lähestyttävään paikkaan. Yksiselitteinen ja selkeä tiedostojen sijainti mahdollistaa sen, että koulutuksissa voidaan viitata aina samaan ajantasaiseen paikkaan. Materiaalin sijainti tulee myös kertoa osana perehdytystä. VDA (2018) vaatimuksena on koulutuksen ja tietoisuuden osalta suorituskykymittarin, joka sisältää käyttäjien koulutuksen ja tietoisuuden. Suorituskykymittarin tarkemmat määreet ovat kuvattu kuviossa kaksi.

Toisena kehitysehdotuksena on, että koulutuksissa, tietoisuuden vaatimuksissa ja ohjeistuksissa käytetään tehtäväperusteista lähestymistapaa. Kehitysehdotus perustuu ensimmäisen kehitysehdotuksen vaatimuksiin (ISO 27001 2017, 7.2, 7.3; VDA 2018, 7.1, 7.2). Perus tietojärjestelmiä käyttävän käyttäjän ja tuotekehityksessä työskentelevän ja jatkuvasti matkustavan työntekijän tietoturvallisuuden tarpeet ovat hyvin erilaiset, vaikka perusasiat ovat jokaisessa tehtävässä samat. Työtehtäviin perustuva koulutus mahdollistaa myös koulutuksen räätälöimisen koulutuksen kohdeyleisön mukaan, jolloin koulutus on osallistujalle mielekkäämpää.

Kolmantena kehitysehdotuksena on, että mobiililaitteiden ja etätyöhön liittyvät ohjeet tulee päivittää kuvaamaan tämän hetkistä tilannetta ja uhkakuvia. Ohjeistuksen tulee myös sisältää tarvittavat kohdat asiakirjojen suojausluokituksesta. Ohjeistus tulee olla osa määriteltyä prosessia, kun käyttäjät ottavat käyttöön tai vaihtavat laitteita sekä etätyön osalta, kun henkilö saa itselleen etätyöoikeuden. Ehdotus perustuu standardin ISO 27001 (2017) kohtaan A.6.2 ja VDA (2018) kohtaan 8.3 sekä osittain myös kohtaan 6.3. Standardissa määritellään, että mobiililaitteisiin ja etätyöhän on otettava käyttöön turvallisuuskäytännöt, joilla hallitaan mobiililaitteiden riskejä sekä käytännöt, joilla suojataan etätyössä käytettyä, käsiteltyä ja säilytettävää tietoa. VDA:n (2018) vaatimus 7.1 ja 7.2 perustuu standardin (ISO 27001 2017).

Kehitysehdotuksiin tulee käyttää prosessimaista toimintamallia, joka on kuvattu kuviossa kolme. Tarvittavat ohjeet ja suuntaviivat ovat suunniteltu osana opinnäytetyötä. Seuraavat vaiheet ovat ohjeiden toteuttaminen, ohjeiden arviointi ja toiminnan tarkastaminen. Toimintamalli ei toimi, mikäli mallia käytetään vain tietoturvallisuuteen liittyvissä ohjeissa. Malli pitää implementoida osaksi tietoturvallisuuden hallintamallia.

Lähteet

Painetut

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13–14 osittain uudistettu painos. Helsinki: Tammi.

Järvinen, P, Rousku, K. 2017. Työpaikan tietoturvaopas. Helsinki: Alma Talent

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Jyväskylä: Gummerus Kirjapaino Oy

Ojasalo, K., Moilanen T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3., uudistettu painos. Helsinki: Sanoma Pro.

Sähköiset

Avoin tiede ja tutkimus. Käsitteistö. Viitattu 28.12.2017. https://avointiede.fi/keskeiset-kasitteet?inheritRedirect=true

Eduskunta. Hallituksen esitys kansallinen tietosuojalaki. 218. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx

EU yleinen tietosuoja-asetus. 4.5.679/2016.

Jyväskylän Yliopisto: Tapaustutkimus. 2015. Viitattu 29.12.2017. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus

Kiwa inspecta: Turvallisuusjohtajan blogi: Kuinka kehityn turvallisuusjohtamisen priimukseksi? 3.11.2017. Viitattu 27.1.2018. https://www.inspecta.fi/Tiedotus/Uutishuone/uutiset/2017/turvallisuusjohtajan-blogi-kuinka-kehityn-turvallisuusjohtamisen-priimukseksi/

Suomen standardoimisliitto SFS. 2015. SFS-EN ISO 9000 Laadunhallintajärjestelmä. Perusteet ja sanasto. Viitattu 21.4.2018. SFS Online

Suomen standardoimisliitto SFS. 2015. SFS-EN ISO 9001 Laadunhallintajärjestelmä. Vaatimukset. Viitattu 22.4.2018. SFS Online

Suomen Standardoimisliitto SFS. 2017. SFS-ISO/IEC 27000 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Viitattu 30.12.2017. SFS Online

Suomen standardoimisliitto SFS. 2017. SFS-ISO/IEC 27001 Informaatioteknologia. Turvallisuus-tekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Viitattu 30.12.2017. SFS Online

Suomen standardoimisliitto SFS. 2017. SFS-ISO/IEC 27002 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Viitattu 30.12.2017. SFS Online.

Suomen standardoimisliitto SFS. 2018. SFS-ISO 31000 Riskienhallinta. Ohjeet. Viitattu 9.5.2018. SFS Online

Tietosuoja. 2017. Viitattu 1.1.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tietosuojavaltuutetun toimisto. Miten valmistautua EU:n tietosuoja-asetukseen. 04/2017. Viitattu 17.3.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

TISAX. 2017. Viitattu 1.1.2018. http://enx.com/tisax/tisax-en.html

VAHTI. Henkilöstön tietoturvaohje. 2013. Viitattu 20.3.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10229

Vahti. Tietoturvallisuudella tuloksia. 2007 Viitattu 2.4.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229

Valmet Automotive A. 2017. Viitattu 28.12.2017. http://www.valmet-automotive.com/automotive/cms.nsf/pages/indexfin

Valmet Automotive B. Historia. Viitattu 28.12.2017. http://www.valmet-automoti-ve.com/automotive/cms.nsf/pages/1DCDA14CE4E393C7C22577060079C90A?opendocument

Valmet Automotive C: Valmet Automotive ostaa Semconin suunnittelupalvelut Saksassa ja laajentaa tarjontaansa autoteollisuudelle. 2017. Viitattu 28.12.2017. http://www.valmet-automoti-ve.com/automotive/bulletin.nsf/PFBD/198561AEBABF22B4C22580BB0026FF4C?opendocument

Valmet Automotive D. Valmet Automotive valmistaa Mercedes-Benzin seuraavan sukupolven kompaktiautomallia. 2017. Viitattu 28.12.2017. http://www.valmet-

automoti-
ve.com/automotive/bulletin.nsf/PFBD/4F09D226F66A0850C22580EB003927AC?opendocument

Valtionvarainministeriö. JUHTA Vahti yhteishankkeiden materiaali. 13.4.2018. Viitattu 17.4.2018. http://vm.fi/documents/10623/7684324/Kopio+ISO27001_GDPR.xlsx/f3500d8e-e3af-47ee-8c33-f1f7f28dcd7a

VDA. Information Security. 2017. Viitattu 01.01.2018. https://www.vda.de/en/topics/safety-and-standards/information-security/information-security-requirements.html

VDA: Information security assessment. 2018. Viitattu 22.04.2018. https://www.vda.de/dam/vda/publications/2015/information-security-assessment-isa-en/VDA-ISA_EN_4-0-3_2018-02-15.xlsx

Kuviot

Liitteet

Liite 1: Yritystä koskevat vaatimukset ISO 27001: 27001 viitekehyksenä

ISO 27001: 2017		EU GDPR		VDA 4.0	
4	Organisaatio ja toimin-taympäristö	25(1)	Sisäänrakennettu ja oletusarvoinen tietosuoja	1.1	Release of an Information Security Management System (ISMS)
5	Johtajuus	32(2) 25(2)	Käsittelyn turvallisuus Sisään rakennettu ja oletusarvoinen tietosuoja	1.1	Release of an Information Security Management System (ISMS)
6	Suunnittelu	32(2) 25(2)	Käsittelyn turvallisuus Sisään rakennettu ja oletusarvoinen tietosuoja	1.2	IS Risk Management
7	Tukitoiminnot				
8	Toiminta	32(2) 28(1) 28(2) 30(1) (a-g) 30(2) (a-d)	Käsittelyn turvallisuus Henkilötietojen käsittelijä Seloste käsittelytoimista	1.2 1.3	IS Risk Management Effectiveness of the ISMS
9	Suorituskyvyn arviointi	28(3) (c)	Henkilötietojen käsittelijä	1.3	Effectiveness of the ISMS
10	Parantaminen			1.3	Effectiveness of the ISMS
A5	Tietoturvapolitiikka				
A5.1	Johdon ohjaus tietoturvalli-suutta ja tietosuojaa kos-kevissa asioissa			5.1	Information Security Policy
A6	Tietoturvallisuuden organi-sointi				
A6.1	Sisäinen organisaatio	5(1)(f)	Henkilötietoja käsittelyä koskevat periaatteet	6.1 6.2	Assigning responsibility for information security Information Security in projects
A6.2	Mobiililaitteet ja etätyö			6.3	Mobile devices
A7	Henkilöstöturvallisuus				
A7.1	Työsopimuksen ehdot			7.1	Contractual information security obligation of employees
A7.2	Johdon vastuut			23.7.2	Awareness and training of employees
A7.3	Tietoturvatietoisuus			7.1	Contractual information security obligation of employees

A7.4	Kurinpitoprosessi		
A7.5	Työsuhteen päättyminen tai vastuiden muuttuminen		
A8	Suojattavan omaisuuden hallinta		
A8.1	Vastuu suojattavasta omaisuudesta		8.1 Inventory of assets
A8.2	Tietojen luokittelu		8.2 Classification of information
A8.3	Tietovälineiden käsittely		8.3 Storage of information on mobile storage devices
A9	Pääsynhallinta		
A9.1	Pääsynhallinnan liiketoiminnalliset vaatimukset		9.1 Access to networks and network services
A9.2	Pääsyoikeuksien hallinta		9.2 User registration 9.3 Privileged user accounts 23.9.2
A9.3	Käyttäjän vastuut		9.4 Confidentiality of authentication data
A9.4	Järjestelmien ja sovellusten pääsynhallinta		9.5 Access to information and applications
A10	Salaus	25(2) Sisäänrakennettu ja oletusarvoinen tietosuoja 32(2) Käsittelyn turvallisuus	10.1 Cryptography
A10.1	Salauksen hallinta		
A11	Fyysinen turvallisuus ja ympäristön turvallisuus		
A11.1	Turva-alueet		11.1 Security zones 11.2 Protection against external influences and external threats 11.3 Protection measures in the delivery and shipping area 23.11.1
A11.2	Laitteet		11.4 Use of equipment
A12	Käyttöturvallisuus		
A12.1	Toimintaohjeet ja velvollisuudet		12.1 Change management 12.2 Separation of development, test and operational environments
A12.2	Haittaohjelmilta suojautu-		12.3 Protection against malware

	minen		
A12.3	Varmuuskopiointi		12.4 Back-up procedures
A12.4	Kirjaaminen ja seuranta		12.5 Event logging 12.6 Logging administrational activities
A12.5	Tuotantokäytössä olevien ohjelmistojen hallinta		
A12.6	Teknisten haavoittuvuuksien hallinta		12.7 Prosecution of vulnerability (patch management)
A12.7	Tietojärjestelmien auditointinäkökohtia		12.8 Review of information systems
A13	Viestintäturvallisuus		
A13.1	Verkon turvallisuuden hallinta		13.1 Management of networks 13.2 Security requirements for networks/services 13.3 Separation of networks (network segmentation) 23.13.3
A13.2	Tietojen siirtäminen	30(1)(a-g) Seloste käsittelytoimista 30(2)(a-d)	13.4 Electronic exchange of information 13.5 Non-disclosure agreements for information exchange with third parties
A14	Järjestelmien hankkiminen, kehittäminen ja ylläpito		
A14.1	Tietojärjestelmiä koskevat turvallisuusvaatimukset		14.1 Requirements for the acquisition of information systems
A14.2	Kehitys- ja tukiprosessien turvallisuus		14.2 Security along the software development process
A14.3	Testiaineisto		14.3 Management of test data
A15	Suhteet toimittajiin		
A15.1	Tietoturvallisuus toimittajasuhteissa	28(3)(e) Henkilötietojen käsittelijä 28(3)h)	15.1 Risk management in collaboration with suppliers
A15.2	Toimittajien palveluiden hallinta		15.2 Review of service provision by suppliers
A16	Tietoturvahäiriöiden hallinta		

A16.1	Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta	33(3)(b) 33(1) 33(2) 33(3)(a) 33(3)(c) 33(3)(d) 33(5) 34(1)	Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle	16.1 16.2	Reporting system for information security incidents (incident management) Processing of information security incidents
A17	Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia				
A17.1	Tietoturvallisuuden jatkuvuus			17.1	Information Security Aspects of Business Continuity Management (BCM)
A17.2	Vikasietoisuus				
A18	Vaatimuksenmukaisuus				
A18.1	Lainsäädännön ja sopimuksiin sisältyvien vaatimusten noudattaminen			18.1 18.2	Legal and contractual provisions Confidentiality and protection of personally identifiable data
A18.2	Tietoturvallisuuden katselmointi			12.8 18.3 18.4	Review of information systems Audit of the ISMS by independent bodies Efficiency test

Liite 2: Voimassa olevat ohjeet

Poistettu salassapitovaatimuksista johtuen.

Liite 3: Vaatimukset ja voimassa olevat ohjeet

Poistettu salassapitovaatimuksista johtuen.